REMARKS

This is in response to the Official Action currently outstanding with regard to the above-identified application, which Official Action the Examiner has designated as being FINAL.

Claims 1, 2 and 6-8 were pending in this application at the time of the issuance of the currently outstanding FINAL Official Action. By the foregoing Amendment, Applicants propose the cancellation of Claims 1 and 2, without prejudice, and also the amendment of Claims 6-8. Applicant does not propose that any Claims be either added or withdrawn. Accordingly, in the event that the Examiner grants the entry of the forgoing Amendment, Claims 6-8 as hereinabove amended will constitute the claims under active prosecution in this application.

The Claims of this application as they will stand in the event that the Examiner grants the entry of the foregoing Amendment are reproduced above showing the changes made and with appropriate status identifiers as required by the Rules.

More specifically, in the currently outstanding Official Action, the Examiner has:

1. Not re-acknowledged Applicants' claim for foreign priority under 35 US 119 (a) – (d) or (f) or to reconfirmed the receipt of the required copies of the priority documents by the United States Patent and Trademark Office – **Applicants note for the record that these matters were previously attended to by the Examiner in the Official Action of 29 June 2005;**

2. Not reconfirmed that acceptance of the formal drawings filed in this application – **Applicants note for the record that this matter also was attended to by the Examiner in the Official Action of 29 June 2005;**

3. Finally rejected Claims 1-2 and 6-8 under 35 USC 112, first paragraph, as failing to comply with the written description requirement in that the claims contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled relevant art that the inventor(s) at the time that the application was filed had possession of the claimed invention.

4. Finally rejected Claims 1-2 under 35 USC 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant regards as the invention.

5. Indicated that Applicants previous argument is not deemed to be persuasive.

6. Finally rejected Claims 1-2 and 6-8 under 35 USC 103(a) as being unpatentable over Lewis (US Patent No. 6,526,506) in view of Shah (US Patent No. 6,041,325).

No further comment regarding items 1-2 above is deemed to be required in these Remarks.

With respect to item 4, Applicants by the foregoing Amendment have proposed the cancellation of Claims 1 and 2, without prejudice, and have proposed extensive amendments to Claim 6. Furthermore, Applicants have proposed that Claims 7 and 8 be amended so as to depend from amended Claim 6. Applicants respectfully submit that the latter amendments to Claim 6 are fully supported at pages 14-22 of the present specification (copies of which being attached hereto for the convenience of the Examiner).

Applicants respectfully submit that the currently amended claim wording set forth hereinabove is such that the Examiner's rejections have been overcome. This is because the Lewis reference simply does not teach, disclose or suggest the input unit and the transmitting unit of Claim 6 as hereinabove amended. More specifically, as will appear more fully below, Applicants understand the portions of the Lewis reference to which the Examiner has referred in support of his rejection, but nevertheless do not find any of the features of the present invention as claimed hereinabove therein (in particular, the input unit and the transmitting unit). Rather, Applicants view the Lewis reference as disclosing inventions directed to multi-level encryption access points for wireless networks that are unrelated to the present invention.

In this regard, Applicants respectfully submit that it should be understood that as now clarified in the claims of this application in the present invention the only manner in which an authentication-authorizing/rejecting response to a request for authorization by a mobile station can be (an in fact must be) transmitted to the mobile station from the access point device from which authentication has been requested is for an authentication-authorizing/rejecting response to the mobile station's request to be input into the input unit of the access point device for transmission to the mobile station that initiated the request by the transmitting unit. This is because if no input to the input means is specifically provided constituting an authorization-authorizing/rejecting response to the authorization request, an input constituting an authorization-rejecting response is provided to the input means. Applicants respectfully submit that if the foregoing was not clearly set forth previously, that potential ambiguity has been corrected by the foregoing Amendment that is specifically supported by the specification as filed (see specification portion attached hereto).

In particular, the claims of this application as amended above now clearly and definitively indicate that the present invention contemplates that the input unit is a unit by which an authentication-authorizing or and authentication-rejecting response to the authentication request of a particular mobile station to the access device is entered, and further that in the absence of the receipt of such an input for a preselected time following the receipt of an authentication request to the access point device, an authorizing-rejection input is generated by default and input into the input unit for transmission to the requesting mobile station. Thus, it now is unambiguously claimed that the only way that a mobile station can be authenticated for an association procedure with the network is by the input of an authentication-authorization response into the input means (which also is displayed by the display means and transmitted to the mobile station by the transmission means). Furthermore, it is now unambiguously claimed that if an authentication authorizing response is not given, an authenticating- rejecting response is given.

Accordingly, Applicants respectfully submit that the foregoing Amendment addresses and overcomes the Examiner's outstanding concerns regarding the breadth of the previous phraseology of the claims of this application.

In addition, as previously mentioned, the Examiner has admitted that the Lewis reference is limited to the LAN administrator establishing criteria kept in a table or memory from which the access point device determines whether or not a particular mobile station should be allowed access to (i.e., to associate with) a network. In other words, the LAN administrator in the Lewis context may set up the original criteria by which authentication-authorizing decisions are made by the access point device and also is permitted to monitor the historical application of those criteria at various intervals for such adjustment as is deemed to be necessary.

Nevertheless, Applicants still have found nothing in the Lewis reference that teaches, discloses or suggests that an authentication-authorizing response to an authentication request by a mobile station can be responded to affirmatively ***only*** by a direct input to an input means of the access point as herein claimed.

More particularly, Applicants respectfully submit that none of the art presently cited against the claims of this application can fairly be said to teach, disclose or suggest an access point device that receives and displays authentication requests from mobile stations coming into the area of the LAN, and input means that is the ***only*** way that a mobile station's authentication authorizing request can be affirmatively responded via a transmitting means whereby the authentication-authorizing/rejecting input to the input unit is sent back to the requesting mobile station for use in a subsequent association procedure with the network.

The Examiner also still attempts to overcome the limitations of the Lewis reference in the above regards via the Shah reference. In particular, the Examiner asserts that the Shah reference provides direct interactions between service operators and service subscribers via a service management access point. On this basis, it is the Applicants' understanding that the Examiner suggests that "Shah discloses the service management access point can accept instructions from data entry operators to direct the service management system to provision services on intelligent networks. More specifically, with user-friendly icons, a service management system can accept and provision particular service features and generate a report for each data entry operator or for each service used."

Applicants in response again respectfully submit, however, that the problem with the Examiner's analysis in the latter regard does not appear to reside in the fact that the Shah network contemplates displays associated with each of the nodes of the network, nor for that matter with his assertions concerning the diverse capabilities of the network in the Shah context once the fixed and mobile nodes thereof have been established. It rather is Applicants' position that the importance of the present invention arises from its determination as to how a mobile station entering the area of a LAN is to secure permission to establish an association with the LAN in the first instance. Once this association is established, Applicants agree that many and diverse capabilities may be possible. Applicants again respectfully submit, however, that the Shah reference is insufficient to make up for the deficiencies of the Lewis reference *vis a vis* the present invention as hereinabove explained and more definitively claimed than perhaps was previously the case.

Consequently, Applicants respectfully submit that the conclusion is inescapable that the present invention includes authentication request display means that receive and display authentication request information from mobile stations entering the area of the LAN. The Shah network nodes, on the other hand, include displays that can display interactively data being utilized on the established network, but as far as Applicants have been able to determine nothing in the Shah or the Lewis references when taken either alone or in combination with one another teaches, discloses or suggests the authentication request display means of the presently claimed access point.

Similarly, as briefly mentioned above, Applicants believe that even though Lewis seems to suggest some interaction by a LAN administrator with an access point concerning the criteria that must be satisfied in order for the access point to grant a specific mobile station association status with the network. the Lewis reference does not teach disclose or suggest that the only way that a particular mobile station can attain association with a network in the first instance is to first seek authentication authorization from an access point that can only be acted upon via an input to the access point device subsequent to its receipt of that request. In the latter regard and also as mentioned above, the displays and keyboards associated with the nodes of the network in the Shah disclosure do not presently appear to be germane to the present invention as now claimed.

Finally, while it may be true that Shah discloses interactions among the nodes of a network, the fact is that neither Lewis nor Shah teach, disclose or suggest that as a result of an authentication authorization requesting step a requesting mobile station desiring to become a node on the LAN must receive via a transmission means of an access point device a response to the authentication authorizing request that grants to the requesting mobile station the authority to associate itself with the network **based upon instructions inputted to the input unit of the access point device subsequent to its receipt and display of the request as in the present invention as now specifically claimed and stated in the attached portion of the specification as originally filed.**

In view of the foregoing Amendment as explained by the foregoing Remarks, therefore Applicant respectfully submits that this application now is in condition for allowance, or at least in better form for Appeal, in accordance with the provisions of 37 CFR 1.116. Accordingly, entry of the foregoing Amendment, reconsideration and allowance of this Application as hereinabove amended in response to this submission is respectfully requested.

Finally, Applicant believes that additional fees are not required in connection with the consideration of this response to the currently outstanding Official Action. However, if for any reason a fee is required, a fee paid is inadequate or credit is owed for any excess fee paid, you are hereby authorized and requested to charge and/or credit Deposit Account No. **04-1105**, as necessary, for the correct payment of all fees which may be due in connection with the filing and consideration of this communication.

Respectfully submitted,

Date: November 3, 2008

By: David A Tucker
David A. Tucker
Reg. No. 27,840
Attorney for Applicant(s)

EDWARDS ANGELL PALMER & DODGE, LLP
P.O. Box 55874
111 Huntington Avenue
Boston, MA 02205
(617) 517-5508

Hereinafter, the operations of the authentication method for the access point device configured as described above will be described.

Here, description will be given of the sequences for the case where a mobile station is turned on or otherwise operated to perform the authentication and association procedures so that the datalink connection with the access point device 18 is established, and for the case where the authentication is rejected.

Assume here that the mobile station MT1 in Fig. 5 described above is the mobile station to perform the authentication processing, and the mobile stations MT2, MT3, and MT4 have already completed the association with the access point device 18 for established datalink.

Initially, referring to Figs. 2 and 4, description will be given of the case where the mobile station MT1 performs the authentication procedure and the network-administering user authorizes the authentication, followed by the association procedure to establish datalink with the access point device 18.

Fig. 2 is a diagram showing the control sequence of the authentication procedure in the case of authorized authentication.

The mobile station MT1 is turned on or otherwise operated to send to the access point device 18 an authentication

Basis of the Claims
Original description 1/9

request message。1 for initiating the authentication procedure by the Shared Key Authentication method.

In the access point device 18, the authentication/association processing means 13 receive this message through the radio communication processing means 12. At AP authentication processing 1 (see the numeral 20 in Fig. 2), the authentication/association processing means 13 make a numerical operation in accordance with the WEP (Wired Equivalent Privacy)-PRNG (Pseudorandom Number Generator) algorithm by using the Initialization Vector and Secret Key values as the parameters. Here, the Initialization Vector and Secret Key values can be arbitrarily determined on each execution of this authentication procedure. The authentication/association processing means 13 thereby obtain a 128-octet uniquely-determined Challenge Text value, and send an authentication response message 1 including this value to the mobile station MT1 through the radio communication processing means 12.

Next, at MT authentication processing 21, the mobile station MT1 receiving this authentication response message 1 ciphers the included Challenge Text value in accordance with the WEP cipher algorithm by using the Shared Secret Data and Initialization Vector as the parameters. The resulting value and the Initialization Vector are included into an authentication request message 2, which is returned to the access point device 18. Moreover, in the access point device 18, the authentication/association processing means 13 receive this message through the radio communication processing means 12. At AP authentication processing 2(see the numeral 22 in Fig. 2), the authentication/association processing means 13 decoded the received ciphered Challenge Text value based on the Initialization Vector which is received concurrently and the Shared Secret Data which is known in advance. The result is compared with the original Challenge Text value stated before, and if identical, the authentication/association processing means 13 execute the procedure of AP authentication processing 3 (see the numeral 23 in Fig. 2). The steps S30-33 in the flow of Fig. 4 show this procedure.

Fig. 4 is a flowchart showing the access point authentication processing described above.

In this procedure, the authentication/association processing means 13 in the access point device 18 initially notify the authentication request display means 16 of authentication wait (step S30). At the same time, the authentication/association processing means 13 start an authentication wait timer set at an arbitrary time (step 31), entering a wait for authentication input (step S32). Meanwhile, the authentication request display means 16 informed of the authentication wait immediately notify the network-administering user of the presence of an authentication-requesting mobile station, through a display device, a loudspeaker, or the like.

Here, the authentication/association processing means 13, if receive a notification from the authentication input means 15 of an authentication-authorizing input made by the network-administering user inputting an authentication authorization before the timeout of the authentication wait timer, send an authentication response message 2 indicating the authorized authentication to the mobile station MT1 through the radio communication processing means 12 (step S33).

Returning to Fig. 2, the mobile station MT1 having received this authentication response message 2, since the result is of authorization, enters the subsequent association procedure to send an association request message to the access point device 18.

Here, in the access point device 18, the authentication/association processing means 13 receive this message through the radio communication processing means 12. Then, at the association processing (see the numeral 24 in Fig. 2), the authentication/association processing means 13 identify the mobile station MT1 by the SSID (Service Set Identifier) in the association request message, and determine whether or not to authorize the association in accordance with a predetermined association authorization rule. If authorize, the authentication/association processing means 13 send an

3/9

association response message that indicates the authorized association to the mobile station MT1 through the radio communication processing means 12. Reception of this association response message by the mobile station MT1 establishes the datalink between the mobile station MT1 and the access point device 18, allowing data communication thereafter.

Next, referring to Figs. 3 and 4, description will be given of the case where authentication is rejected of the mobile terminal MT1 by the network-administering user in the authentication procedure, and the case where the authentication wait timer goes time-out to reject the authentication automatically.

Fig. 3 is a diagram showing the control sequence of the authentication procedure for rejected authentication/timeout.

In Fig. 3, the mobile station MT1 is turned on or otherwise operated to send to the access point device 18 an authentication request message 1 for initiating the authentication procedure by the Shared Key Authentication method.

In the access point device 18, the authentication/association processing means 13 receive this message through the radio communication processing means 12. Then, at the AP authentication processing 1 (see the numeral 25 in Fig. 3), the authentication/association processing means

13 performs a numerical operation in accordance with the WEP (Wired Equivalent Privacy)-PRNG (Pseudorandom Number Generator) algorithm by using the Initialization Vector and Secret Key values, which can be arbitrarily determined upon each execution of this authentication procedure, as the parameters. The authentication/association processing means 13 thereby calculate a 128-octet uniquely-determined Challenge Text value, and send the authentication response message 1 including this value to the mobile station MT1 through the radio communication processing means 12.

Then, at the MT authentication processing (see the numeral 26 in Fig. 3), the mobile station MT1 receives this authentication response message 1, and ciphers the Challenge Text value included therein in accordance with the WEP cipher algorithm, with the Shared Secret Data and Initialization Vector as the parameters. The resulting value and the Initialization Vector are included into an authentication request message 2, which is returned to the access point device 18. Besides, in the access point device 18, the authentication/association processing means 13 receive this message through the radio communication processing means 12. At the AP authentication processing 2 (see the numeral 27 in Fig. 3), the authentication/association processing means 13 decode the ciphered Challenge Text value received, based on the Initialization Vector received concurrently and the Shared

7/9

Secret Data known in advance. The result is compared with the original Challenge Text value stated before, and if identical, the authentication/association processing means 13 execute the procedure of the AP authentication processing 3 (see the numeral 28 in Fig. 3). This procedure is shown as the steps S30-S32, and S34 of the flow in Fig. 4.

In this procedure, the authentication/association processing means 13 in the access point device 18 initially notify the authentication request display means 16 of an authentication wait (step S30). At the same time, the authentication/association processing means 13 start the authentication wait timer set at an arbitrary time (step S31), entering a wait for authentication input (step 32). Meanwhile, the authentication request display means 16 informed of the authentication wait immediately notify the network-administering user of the presence of an authentication-requesting mobile station, through a display device, a loudspeaker, or the like.

Here, the authentication/association processing means 13, if receive a notification from the authentication input means 15 of an authentication-rejecting input made by the network-administering user inputting an authentication rejection before the timeout of the authentication wait timer, send an authentication response message 2 that indicates the authentication rejection to the mobile station MT1 through the

8/9

radio communication processing means 12 (step S34). Similarly, when the authentication wait timer goes time-out during the authentication input wait (step S32), the authentication/association processing means 13 send the authentication response message 2 that indicates the authentication rejection to the mobile station MT1 through the radio communication processing means 12 (step 34).

Returning to Fig. 3, the mobile station MT1 having received this authentication response message 2 cannot enter the subsequent association procedure since the result is of rejection. If necessary, the mobile station MT1 notifies its user of the failed authentication (see the numeral 29 in Fig. 3). Thus, in this case, the mobile station MT1 is incapable of data communication.

Incidentally, the WEP algorithm mentioned here is defined in the RC4 technology by RSA Data Security Inc. Besides, the association processing (see the numeral 24 in Fig. 2) is identical to the association procedure defined in IEEE 802.11.

Moreover, the arbitrary time set the authentication wait timer is set at can be arbitrarily determined by the network-administering user, as a value appropriate in terms of the time that is required from the network-administering user recognizing the presence of an authentication-requesting mobile station through the authentication request display means to the user inputting an authorization through the authentication input means to authorize the mobile station.

As has been described above, in the present embodiment, the access point device 18 includes the authentication request display means 16 and the authentication input means 15. When a mobile station in the area performs the authentication procedure before the initiation of the association procedure, the authentication request display means 16 make a notification of the authentication-requesting mobile station in the area so that the access point device 18 obtains the final authorization of the authentication procedure from the LAN-administering user. The network administrator notified provides an authentication-authorizing or -rejecting instruction to the authentication-requesting mobile station through the authentication input means 15. In the pre-association authentication procedure of a mobile station on a wireless LAN system which is physically invisible and therefore subject to attacks from network intruders with evil intent, the access point device 18 allows the network-administering user to see who is making the association before granting authorization, instead of the automatic authorization by the access point. This means a significant improvement in security level.

Moreover, in a wireless LAN system that implements the Shared Key Authentication procedures defined as an option in IEEE 802.11, this authentication procedure can be put into